	Application No.	Applicant(s)
Notice of Allowability	09/955,902	STOJANCIC ET AL.
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *interview on 5/12/2005*.

2. ☒ The allowed claim(s) is/are *1,7,9,11,13,15,17,18,27,29,31,33-36,38-48,50-60 and 62-72*.

3. ☒ The drawings filed on *18 January 2002* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All   b) ☐ Some*   c) ☐ None   of the:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date ~~5/16/2005~~ 5/12/05

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as

provided by 37 CFR 1.312. To ensure consideration of such an amendment, it

MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone

interview with Craig G. Holmes (Reg. No: 44,770) on 5/12/2005.

This application has been amended as follows:

IN THE CLAIMS

Cancel claims 6, 37, 49 and 61 without prejudice.

Replace claim 1, 7, 11, 13, 15, 34 – 36, 38, 39 – 41, 50 – 54 and 63 – 66

as follows.

Claim 1:   A method for encryption and decryption of electronic messages

based on an encryption protocol, the method comprising the

computer-implemented steps of:

        receiving a first electronic message that is encrypted according to

    the encryption protocol;

generating at least one part of a second electronic message, based

on at least the first electronic message, a modular operation that is based

on two applications of Montgomery's method, a first operand, a second

operand, ~~and~~ a modulus, <u>and a modular reduction using a negative</u>

<u>multiplicative inverse of the modulus,</u> and wherein the step of generating

the second electronic message includes the computer-implemented steps

of:

generating a first constant <u>(R)</u> based on the modulus <u>(M) by</u>

<u>selecting a second constant (W) such that $W \geq 4M$ and</u>

<u>determining the first constant (R) according to the</u>

<u>expression $R = W^2 (mod(M))$;</u>

in a first application of Montgomery's method, determining an

intermediate result based on at least Montgomery's method

for the modular operation, the first operand, and the first

constant; and

in a second application of Montgomery's method, determining and

storing in memory a final result that comprises the at least

one part of the second electronic message, based on at

least Montgomery's method for the modular operation, the

intermediate result, and the second operand.

Claim 7:   The method of Claim 6 1, wherein the second constant (W)

is not a power of two.

Replace claim 11 Line 3 with the following:

        a the negative multiplicative inverse of the modulus

Replace claim 13 Line 3 – 4 with the following:

        a the negative multiplicative inverse of the modulus

Replace claim 15 Line 3 with the following:

        a the negative multiplicative inverse of the modulus

Claim 34:   A computer-readable medium carrying one or more sequences of

instructions for encryption and decryption of electronic messages based on an

encryption protocol, which instructions, when executed by one or more

processors, cause the one or more processors to carry out the steps of:

        receiving a first electronic message that is encrypted according to the

encryption protocol;

generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and a modular reduction using a negative multiplicative inverse of the modulus, and wherein the instructions for generating the second electronic message further comprise instructions which, when executed by one or more processors, cause the one or more processors to carry out the steps of:

> generating a first constant (R) based on the modulus (M) by selecting a second constant (W) such that $W \geq 4M$ and determining the first constant (R) according to the expression $R = W^2 (mod(M))$;

> in a first application of Montgomery's method, determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

> in a second application of Montgomery's method, determining and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand.

Claim 35:   An apparatus for encryption and decryption of electronic messages based on an encryption protocol, comprising:

> means for receiving a first electronic message that is encrypted according to the encryption protocol;

means for generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, ~~and~~ a modulus, <u>and a modular reduction using a negative multiplicative inverse of the modulus,</u> and wherein the means for generating the second electronic message further comprises:

means for generating a first constant <u>(R)</u> based on the modulus <u>(M) by selecting a second constant (W) such that $W \geq 4M$ and determining the first constant (R) according to the expression R $= W^2 \, (mod(M))$</u>;;

means for determining, in a first application of Montgomery's method, an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

means for determining, in a second application of Montgomery's method, and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand.

Claim 36:   An apparatus for encryption and decryption of electronic

messages based on an encryption protocol, comprising:

an interface;

a processor coupled to the interface and receiving information from the

interface; and

one or more stored sequences of instructions which, when executed by

the processor, cause the processor to carry out the steps of:

receiving a first electronic message that is encrypted according to the

encryption protocol;

generating at least one part of a second electronic message, based on at

least the first electronic message, a modular operation that is based on two

applications of Montgomery's method, a first operand, a second operand, and a

modulus, and a modular reduction using a negative multiplicative inverse of the

modulus, and wherein the instructions for generating the second electronic

message further comprise instructions which, when executed by the processors,

cause the processor to carry out the steps of:

generating a first constant (R) based on the modulus (M) by selecting a

second constant (W) such that $W \geq 4M$ and determining the first

constant (R) according to the expression $R = W^2 (mod(M))$;;

in a first application of Montgomery's method, determining an intermediate

result based on at least Montgomery's method for the modular

operation, the first operand, and the first constant; and

in a second application of Montgomery's method, determining and storing

in memory a final result that comprises the at least one part of the

second electronic message, based on at least Montgomery's

method for the modular operation, the intermediate result, and the

second operand.

Claim 38:   The apparatus of Claim 37 36, wherein the second constant

(W) is not a power of two.

Replace claim 39 Line 3 with the following:

a the negative multiplicative inverse of the modulus

Replace claim 40 Line 3 with the following:

a the negative multiplicative inverse of the modulus

Replace claim 41 Line 3 – 4 with the following:

a the negative multiplicative inverse of the modulus

Claim 50:   The computer-readable medium of Claim 49 34, wherein the

second constant (W) is not a power of two.

Replace claim 51 Line 4 with the following:

a the negative multiplicative inverse of the modulus

Replace claim 52 Line 3 – 4 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Replace claim 53 Line 4 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Replace claim 54 Line 4 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Claim 62:   The apparatus of Claim ~~61~~ 35, wherein the second constant

(W) is not a power of two.

Replace claim 63 Line 3 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Replace claim 64 Line 3 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Replace claim 65 Line 3 – 4 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Replace claim 66 Line 3 – 4 with the following:

a ~~the~~ negative multiplicative inverse of the modulus

Allowable Subject Matter

Claims 1, 7, 9, 11, 13, 15, 17 – 18, 27, 29, 31, 33 – 36, 38 – 48, 50 – 60 and 62 – 72 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 1 and subsequent dependent claims.

The CPA fails to teach or suggest a system for providing the dual applications of Montgomery's method generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, a modulus, and a modular reduction using a negative multiplicative inverse of the modulus, and wherein the step of generating the second electronic message includes the computer-implemented steps of:

generating a first constant (R) based on the modulus (M) by selecting a second constant (W) such that $W \geq 4M$ and determining the first constant (R) according to the expression $R = W^2 (\mathrm{mod}(M))$;

in a first application of Montgomery's method, determining an

intermediate result based on at least Montgomery's method

for the modular operation, the first operand, and the first

constant; and

in a second application of Montgomery's method, determining and

storing in memory a final result that comprises the at least

one part of the second electronic message, based on at

least Montgomery's method for the modular operation, the

intermediate result, and the second operand.

Claims 34 – 36 and subsequent dependent claims would also be
allowable for the reasons stated above

Any comments considered necessary by applicant must be submitted no
later than the payment of the issue fee and, to avoid processing delays, should
preferably accompany the issue fee. Such submissions should be clearly labeled
"Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from
the examiner should be directed to Longbit Chai whose telephone number is
571-272-3788. The examiner can normally be reached on Monday-Friday
8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100